STATEMENT BY

JACQUELINE SIMON
PUBLIC POLICY DIRECTOR
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO

BEFORE

THE SUBCOMMITTEE ON FEDERAL WORKFIRCE AND AGENCY ORGANZIATION

HOUSE COMMITTEE ON GOVERNMENT REFORM

REGARDING

THE FEDERAL FAMILY HEALTH INFORMATION TECHNOLOGY ACT OF 2006 (H.R. 4859)

ON

JUNE 13, 2006

I. INTRODUCTION

My name is Jacqueline Simon, and I am the Public Policy Director of the American Federation of Government Employees (AFGE), AFL-CIO. On behalf of the 600,000 federal employees represented by AFGE who serve the American people across the nation and around the world, I thank you for the opportunity to testify on the Federal Family Health Information Technology Act of 2006 (H.R. 4859).

At the outset, Mr. Chairman, let me thank you for your personal attention to this legislation and the access that you have provided to AFGE during your deliberations. We know that the plan is well-intentioned.

The Federal Family Health Information Technology Act of 2006 proposes to allow that every participant of the Federal Employees Health Benefits Program (FEHBP) maintain a personal electronic health record (EHR). It would also require every insurance company and health care provider to create and maintain electronic records for each individual covered by an FEHBP plan. The rationale for the legislation is to overcome the costs and problems that derive from the fact that current methods of compiling and tracking medical data are so fragmented that they give rise to medical errors, duplicative testing, and incomplete medical histories. There is no question that these problems have the potential to adversely affect the quality of health care, and in some instances may compromise patient safety.[1] Another impetus is to respond to the frustrations and unnecessary costs borne by those who, because they must see multiple doctors, are sometimes forced to repeat tests and procedures because of lost or misplaced records. Requiring electronic medical records under the new bill is an attempt to address these issues and ultimately improve health care delivery for patients.

Although health information technology may assist physicians and other medical professionals in reducing medical errors, my testimony will focus on the many questions federal employees have regarding privacy, costs, accuracy, access, and the potential difficulties that may emerge from the implementation and maintenance of electronic health records in the context of FEHBP's current structure and regulatory framework.

II. CONCERNS

While supporters of the bill have maintained their belief that using electronic technology to compile and transfer medical data could prevent "tens of thousands of patients" from dying every year due to medical errors, it seems premature to make such claims without first testing the advantages and disadvantages of this new initiative in a pilot project within FEHBP. There is

[1] GAO-06-346T, "Health Information Technology: HHS is Continuing Efforts to Define a National Strategy" (March 15, 2006).

precedent for making dubious claims on behalf of FEHBP in the context of national health policy. To the extent that FEHBP is used as a model for other federal health insurance programs, it is important that great care be taken to make sure that the terms for adoption of electronic technology is accomplished in a way that justifies its costs and minimizes its risks.

AFGE cannot assume that using EHRs will be a "cure-all" to the countless problems in American health care generally or even FEHBP specifically. According to the Institute of Medicine, the federal government has a central role in shaping nearly all aspects of the health care sector as a regulator, purchaser, health care provider, and sponsor of research, education, and training.[2] Given the federal government's significant influence in the health care industry, it is crucial that it utilize adequate safeguards and always keep the best interest of the patient as the primary focus in its policies, particularly in the context of implementing this proposed legislation. Because of the political prominence of FEHBP, failure to take these precautions could set dangerous precedents that might affect health care delivery not just for federal employees, retirees, and their dependents, but for the entire country as well.

A. Privacy: Promises Are Not Enough

Although physicians have always been bound by a code of conduct requiring that they protect the privacy of their patients, in recent years health information has come into use by many organizations and individuals who are not subject to medical ethics codes.[3] The ubiquitous use of computers has made access to confidential medical records much easier, and much more vulnerable to exploitation. However much potential digitizing federal employee health records has to improve health care by avoiding errors and helping providers base treatment on more complete information, health care automation could create problems for the patient that extend far beyond the hospital or clinic. There is legitimate concern that electronic health records will not be secure from either loss or unauthorized access, as the recent theft of data from an employee of the Department of Veterans Affairs attests. A recent survey of more than 1,000 consumers found that 44% rank overcoming privacy and security issues as the "top challenge" in implementing EHRs.[4] Yet, 86% of respondents are "somewhat or very concerned about the health industry's ability to protect the privacy of personal health information in deploying EHRs."[5]

Although the "privacy rule," established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires medical professionals to make

[2] GAO-06-346T, "Health Information Technology: HHS is Continuing Efforts to Define a National Strategy" (March 15, 2006).
[3] www.epic.org/privacy/medical
[4] Health Industry Insights citing *Consumer Attitudes Toward EMRs, EHRs and the Privacy of Health Information*. (Marc Holland)
[5] Health Industry Insights citing *Consumer Attitudes Toward EMRs, EHRs and the Privacy of Health Information.* (Marc Holland)

reasonable efforts to limit the disclosure of medical information to the "minimum necessary, " this rule is not absolute. While insurance companies and providers are well aware of their duties under HIPAA, it is questionable if all medical personnel understand the various restrictions surrounding "medical privacy" and how to treat confidential data.[6] As the Electronic Privacy Information Center has correctly stated, "the regulatory regime for protecting privacy of health information is complex and fragmented."[7] Although there is a federal mandate on protecting health information, there are also existing state laws which protect the confidentiality of patient information to varying degrees as well.[8] There are also protections that apply only to specific medical conditions or types of information, such as information related to HIV/AIDS or substance abuse treatment.[9] Some medical professionals may have already been mystified by the complexity of HIPAA alone. Navigating state law and other regulations in conjunction with HIPAA seems to further obscure what is truly considered private.

Even if HIPAA and its regulations were adequate the current reluctance to enforce federal regulations makes the bill's conformance with HIPAA almost an irrelevancy. *The Washington Post* reported last week that in the three years since HIPAA's enactment, no fines have been imposed even though 19,420 grievances have been filed. The grievances included allegations that "personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained, (and), patients were frustrated getting their own records." Although insurance companies, hospitals, health plans, and doctors were reported to be quite satisfied with the lax enforcement, patients and patient advocates were not. Especially troubling for federal employees, the representative from the Department of Health and Human Services (HHS) whose office is responsible for enforcing the law is quoted saying that "challenges with our resources investing compliance" was part of the explanation for why more has not been done to enforce privacy complaints.

Federal employees are more intimately aware than anyone that inadequate funding for agency staffing and political bias have made carrying out regulatory enforcement a low priority. They will not find credible promises that the Office of Personnel Management (OPM) will enforce HIPAA-like privacy protections, and they will not find credible assurances that the data or the program will be implemented in ways that serve their interests.

Privacy is such an enormous concern because one's health record can often reveal some of the most intimate and personal aspects of a federal employee's life. Medical records include the details of family history, genetic testing,

---

[6] http://www.hhs.gov/ocr/hipaa/consumer_rights.pdf
[7] www.epic.org/privacy/medical
[8] www.epic.org/privacy/medical
[9] www.epic.org/privacy/medical

diseases and treatments, illegal drug use, sexual orientation and practices, and testing for sexually transmitted diseases. Subjective remarks about a patient's demeanor, character, and mental state are sometimes a part of the record as well.[10] The proposed legislation does not address how variations in business policies, state laws that affect privacy and security practices, including those related to HIPAA, and other challenges to health information exchange could result in the mishandling or misinterpretation of patient health records—even assuming that HIPAA protections were enforced.

While the system may be designed to facilitate collaboration and improve medical care, the legislation establishes no safeguard to ensure that individual confidentiality will not be compromised. There are no direct restraints on who has access to a patient's health and/or medical information, what information from a patient's health records will and will not be available for viewing, or if there will be an electronic paper trail created by anyone who looks at the records. If the federal government cannot commit to genuinely impregnable firewalls to protect privacy and control access, then no federal employee's health information should be placed in an electronic record without his or her affirmative permission, permission that must be able to be withdrawn and given entirely at will.

B. Costs: Who Will Pay?

One of the most troubling aspects of the proposed Federal Family Health Information Technology Act of 2006 is its advocates' insistence that the adoption of electronic health records will result in significant health care cost savings, and that these savings will be passed on to either agencies, enrollees, or both. While there might be some clinical savings and gains from greater physician productivity as a result of using EHRs, there is every reason to believe that most or all of these savings will be off-set by higher administrative costs. *The added administrative costs are real and the savings are only hoped-for projections of future savings.* Even if money is saved by better coordination of care and integration of recommendations for preventive services that will help to avoid or greatly diminish the costly deterioration in a patient's condition, forcing every practice to submit yet another set of medical data will be extremely costly. Direct providers of medical care already have to collect their own records (as required under standard medical practice protocols and malpractice insurance requirements) and submit bills to insurers and/or patients. This legislation will essentially force them to complete yet another reporting requirement. Although there are provisions for temporary financial "incentives" or subsidies to providers, what happens when the period for these payments expires? Small medical practices will become so overwhelmed, physically and financially, by having to duplicate their efforts to document a patient's health and medical history, that the

[10] "Protecting Privacy in Computerized Medical Information," Digest of OTA Report (September 1993).

end result might cause them to drop their insurance carriers simply because they will not tolerate any more paperwork. More than 67% of consumers who were surveyed agree that electronic medical records will not "materially reduce" the cost of health care, even if it favorably impacts the delivery of care.[11]

While the Christiana Medical Center in Delaware was cited as an example in the previous hearing on this legislation to advertise the cost-saving results that health information technology can produce, it must be recognized as an unusual and special case because just one health plan and one medical center cover a huge percentage of one community's population. A more useful and realistic test of the efficiency and cost-saving potential of EHRs needs to be performed on scattered, small medical practices since they are a far more common phenomenon within FEHBP. Indeed, the largest FEHBP plan, the Blue Cross-Blue Shield Standard Option, includes nationwide networks of hundreds of thousands of providers. Testing cost effectiveness of EHRs on small medical practices will measure the impact of increased administrative costs for developing and maintaining electronic records, as well as the size of start-up costs. In fact, a recent study found that "start-up costs for an electronic health records system cost about $44,000 per physician in small-group practices."[12]

The start-up costs to fund EHRs in the federal government will likely be just as significant, but the government may not be able to finance those costs. The Federal government has chosen to fund the initial phases of implementation by expending the remainder of the one percent of reserves not currently used for other administrative costs by OPM. *AFGE strongly opposes the use of the FEHBP reserves for this purpose.* To propose to use the reserves to fund electronic medical records directly contradicts the pledge to have insurance carriers bear the initial costs of system, as the reserves are paid by agencies and enrollees.

Although OPM claims that this money will be recouped from the savings that the new technology system will bring, there is no empirical evidence to suggest that this program will ever bring any savings, and even if it did, there is nothing to suggest when these savings would begin to accrue.

Finally, AFGE strongly disagrees with the contention that Blue Cross-Blue Shield or any other health insurance carrier will effectively be prevented from passing along the costs of the electronic medical records initiative to plan participants. FEHBP carriers have won a statutory exemption from application of the government's Cost Accounting Standards (CAS) that are applied to other large federal health care contracts.

---

[11] Health Industry Insights citing *Consumer Attitudes Toward EMRs, EHRs and the Privacy of Health Information*. (Marc Holland)

[12] **Medscape** citing **The Nation's Health**: "Improved Medical Technology Could Affect Health, Lower Cost," by Kim Krisberg (November 11, 2005).

The government's CAS are designed, among other things, to ensure that contractors appropriately estimate, accumulate and report their contract costs in a consistent manner, as well as allocate the costs that involve their non-government customers. Without the protections afforded by CAS, there is literally no way to ensure that FEHBP's carriers are prevented from assigning the costs associated with carrying out the electronic medical records initiative to the plan participants. At a minimum, it is necessary to remove the exemption from the application of CAS from all FEHBP carriers in order to provide the government with the ability to enforce its promise to federal employees and retirees that the cost of this initiative will not be paid by participants.

C. Opt-Out

Motivating federal employees to participate voluntarily in the use of electronic health records will undoubtedly present a challenge, since many individuals have legitimate apprehensions about the security, effectiveness and usefulness of such a practice. They need only read the newspaper to learn about the government's failure to enforce HIPAA, or the unfortunate theft of millions of veterans' financial and medical information to justify their unease. Forcing an individual to put his or her medical records on-line will foster enormous anger and resentment among federal employees, and leave them feeling as if they are being forced to sacrifice control over the privacy, access, or distribution of their medical records as part of the price of federal employment. They will fear that their records may fall into the hands of current or future employers who could misinterpret information and use it against them without their ever knowing what transpired. They will know that the Administration places a low priority on regulatory enforcement, and they will doubt the efficacy of electronic records as a health care cost reduction tool. Finally, even for those who may be persuaded that there will be a cost or quality of health care rationale for electronic medical records, there will be serious questions about privacy and accuracy.

We believe that this program should be started as a pilot or demonstration project within FEHBP, and be open to a small population of volunteers. If projections of savings are realistic, insurance companies should be eager to participate and should be willing to subject themselves to the government's CAS in order to prove that the savings are real. Once the pilot has had a sufficient period of time to allow objective evaluation of its costs and benefits, the decision can be made whether to expand it. If it is as successful as the bill's advocates believe it will be, it is likely that both insurance companies and federal employees will be comfortable with participating.

D. Efficiency

Providing accurate and comprehensive health care information is critical to the physician-patient relationship and the quality of health care delivery. In some instances, we are persuaded that using EHRs can facilitate progress in this area.

However, there is a great deal of evidence suggesting that the use of electronic medical records can actually cause a breakdown in the communication between physician and patient, and in many instances can disrupt the delivery of efficient and quality health care.

In a study examining the way that physicians use computers to collect and interpret patient health records in the examination room, results showed that technology can be extremely disruptive, causing a great deal of tension between the control of the EHR process and conduct of a medical interview.[13] Physician behavior was described as "pre-occupied," with attention largely focused on the computer monitor and only intermittently on the patient. The patient visits were characterized by "frequent periods of silence," and the use of EHRs often caused a change in the physician's work style from "conversational" to "block" style.[14]

The study further found that this type of verbal distancing from the patient does in fact negatively affect the patient-doctor relationship, particularly in the psychosocial and emotional realm. The doctor's constant attention to the screen seemed to suggest to the patient that his or her issues were unimportant or that there was a lack of interest or unwillingness on the part of the physician to engage in interaction. This often caused the patient to be emotionally unresponsive and avoid full disclosure, which in turn greatly inhibited the doctor's ability to properly diagnose and/or treat that patient.[15]

The observational study also found that while the use of electronic medical records strengthened the physician's ability to gather data, there were other unfortunate effects that EHRs had on patient-centered medical care. The benefit of the physician being able to gather data more efficiently was largely undermined because the physician virtually never shared the screen with patients to review medical information that may have affected his or her health (i.e. laboratory test results, patient progress in disease management, understanding of a disease or a specific treatment.)[16] Thus, errors in transmission of information compromised the accuracy of the information in the EHR.

---

[13] Patient Education and Counseling 61 (2006) 134-141: "Electronic Medical Record Use and Physician-Patient communication: An Observational study of Israeli primary care encounters," by Ruth Stashefsy Margalit, Debra Roter, Mary Ann Dunevant, Susan Larson, Shmuel Reis.
[14] Patient Education and Counseling 61 (2006) 134-141: "Electronic Medical Record Use and Physician-Patient communication: An Observational study of Israeli primary care encounters," by Ruth Stashefsy Margalit, Debra Roter, Mary Ann Dunevant, Susan Larson, Shmuel Reis.
[15] Patient Education and Counseling 61 (2006) 134-141: "Electronic Medical Record Use and Physician-Patient communication: An Observational study of Israeli primary care encounters," by Ruth Stashefsy Margalit, Debra Roter, Mary Ann Dunevant, Susan Larson, Shmuel Reis.
[16] Patient Education and Counseling 61 (2006) 134-141: "Electronic Medical Record Use and Physician-Patient communication: An Observational study of Israeli primary care encounters," by Ruth Stashefsy Margalit, Debra Roter, Mary Ann Dunevant, Susan Larson, Shmuel Reis

It must be acknowledged that the amount of information that a physician has about a patient at the point of care does not impact the quality of care that the patient receives nearly as much the physician's engagement and responsiveness with the actual patient. Unfortunately, many physicians are not trained to use EHRs and simultaneously maintain a verbal rapport and interpersonal communication with the patient, as they will become focused on one task or the other--but not both. As the Subcommittee considers having all FEHBP participants use electronic medical records, it is critical to consider seriously both the positive and negative implications that can result from such practices, and make decisions about what truly is in the best interest of the patient.

This concludes my statement. I will be happy to answer any questions that the Chairman or other Members of the Subcommittee may have.